

User Requirements:

1. Obtain and utilize your NOAA email address to communicate regarding NOAA issues;
2. You must undergo the appropriate type of suitability check i.e. background investigation process for your level of access. For regular access to the RDHPCS resources, a National Agency Check and Inquiries (NACI) background check is required. You will need to initiate or complete a background check with the NOAA Personnel Security Office (OSY). For additional information see the [suitability check page](#). This can take between 6 -12 weeks to complete - currently it is longer. Once this is complete, your Federal Sponsor will work with the line office's Trusted Agent to forward your OSY clearance email to rdhpcs.aim.help@noaa.gov;
3. You must complete NOAA's annual IT Security Awareness Course (ITSAC) training (1 hour of security training). Access to this course will be emailed to you once you are eligible;
4. You must verify your account information in [AIM](#) annually and agree to all the [RDHPCS policies](#);
5. You must have an approved project request in [AIM](#);
6. You must maintain an active account by logging into the system every 30 days to renew your Proxy Certificate; and
7. If you are a Foreign National (FN), please work with your Foreign National Sponsor to completed the FN Visitor paperwork. Please see the [deemed export website](#) for more information.

Reactive an Account:

1. After 60 days of inactive, the token will be locked and the user will need to reapply for an account through [AIM](#).
2. You must maintain an active account by logging into the system every 30 days to renew your Proxy Certificate. After 30 days, users will be prompted to renew their proxy certificate with their passphrase. Users will have an additional 30 days to renew their proxy certification before the token is locked and they must reapply for an account.
3. Users who cannot remember their passphrase will need to enter it incorrectly until they are prompted to also create a new master certificate and a corresponding new passphrase. During this process of making a new master certificate/passphrase the user will have to go through the certificate signing delay again just as in the steps of first-time login process. They must go through the AIM process.

From:

<https://rdhpcs-common-docs.rdhpcs.noaa.gov/wikis/rdhpcs-common-docs/> - **RDHPCS-Common-Docs**

Permanent link:

https://rdhpcs-common-docs.rdhpcs.noaa.gov/wikis/rdhpcs-common-docs/doku.php?id=prereqs_for_users 

Last update: **2015/10/23 04:05**